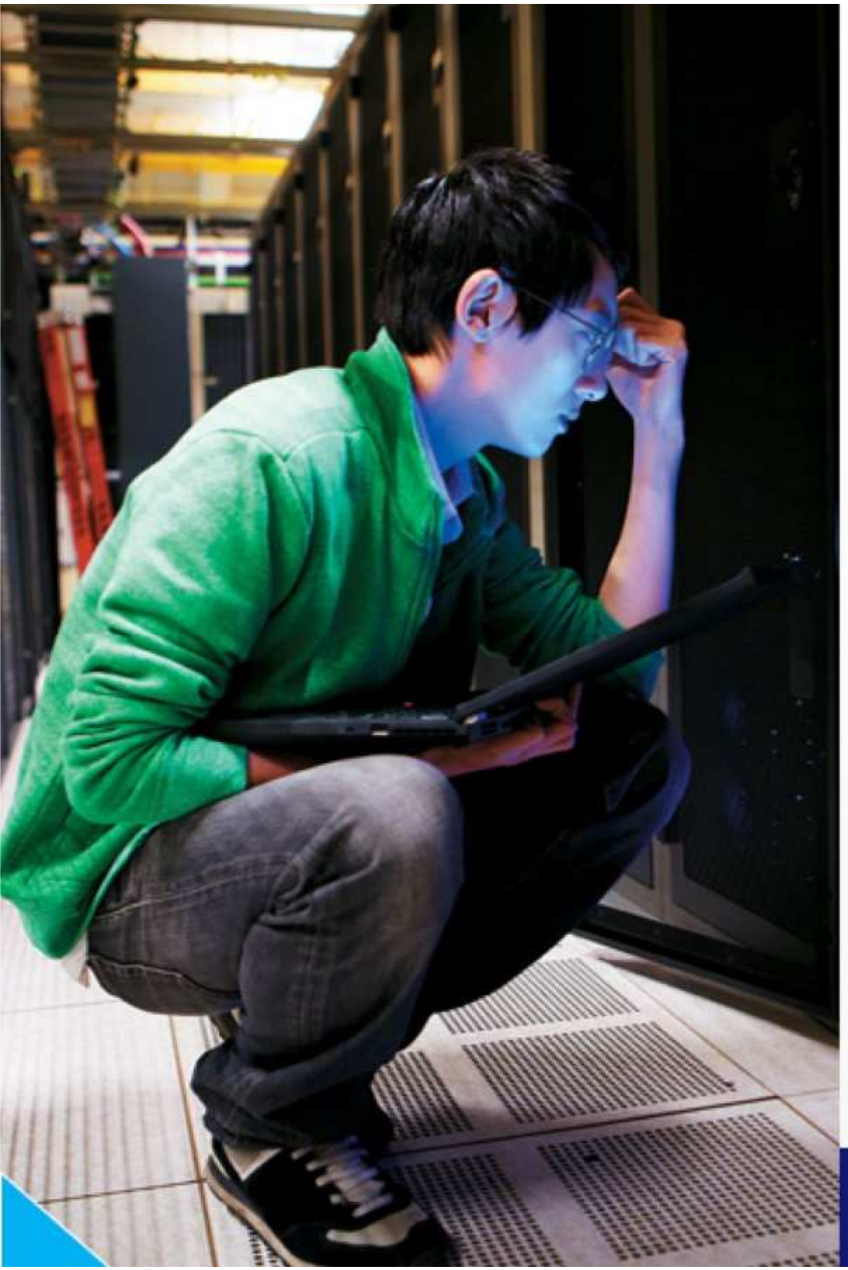


DirectAccess dans Windows Server 2012

Arnaud Lheureux | Architecte Infrastructure
http://aka.ms/arnaud
Stanislas Quastana | Architecte Infrastructure
http://aka.ms/stanislas
Microsoft France

Entreprise / IT / Serveurs / Réseaux / Sécurité

Microsoft tech·days 2013

Accès distants aujourd'hui

- Les utilisateurs ont parfois du mal à accéder aux ressources de leur entreprise à distance
  - Ergonomie des outils discutable
  - Temps d'établissement des connexions
  - Mauvaise formation aux outils
  - Applications non publiables…
- Les postes nomades sont difficilement administrables à distance par les équipes IT

Objectifs de DirectAccess

- Répondre aux nouveaux besoins et usages
- Rendre les utilisateurs plus mobiles
- Se connecter depuis n'importe où
- Rester connecter en permanence
- Travailler plus efficacement

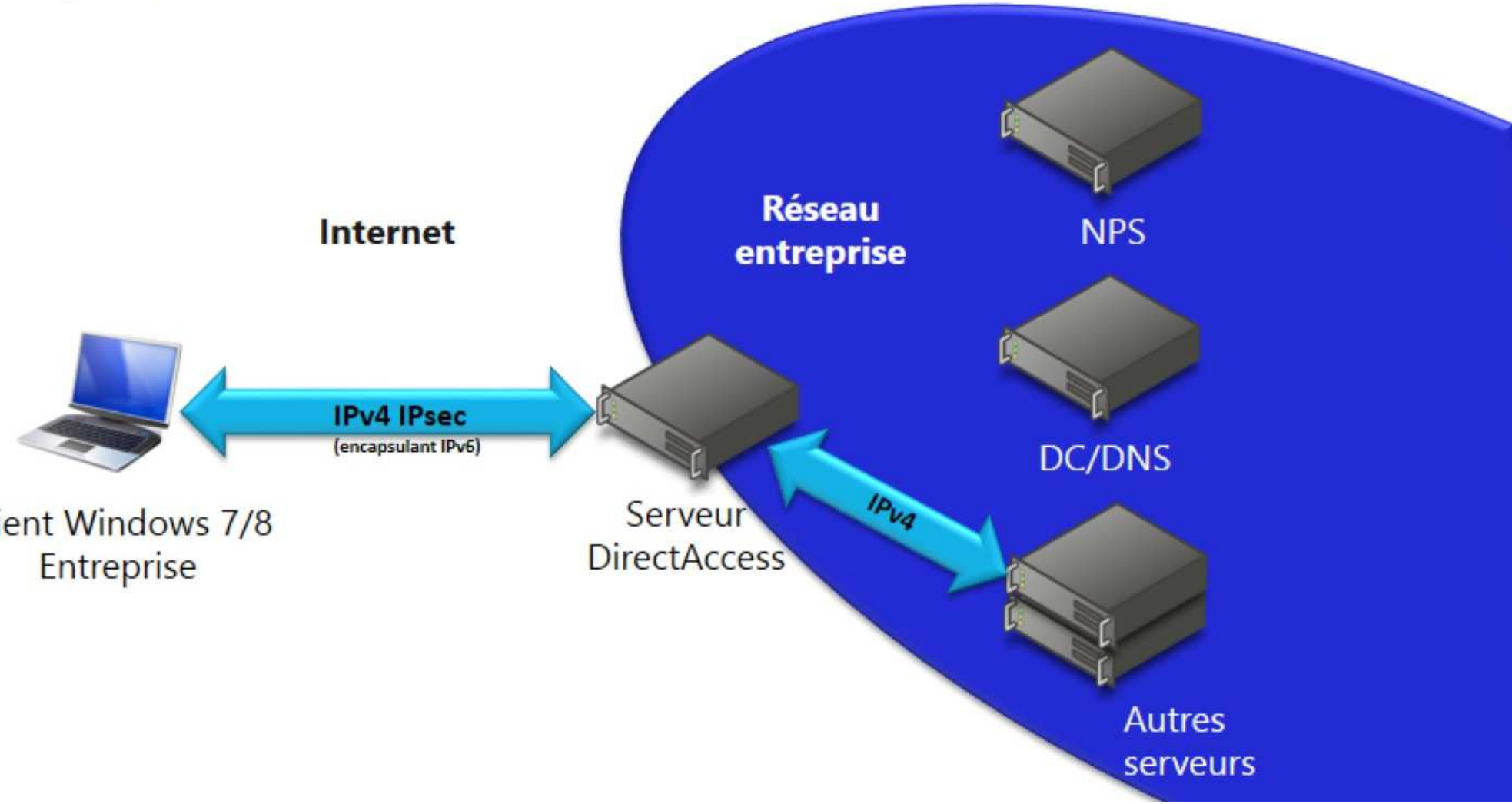
→ Redonner le contrôle logique aux équipes IT qui ont perdu le contrôle physique des postes

DirectAccess en quelques points

- Accès distant transparent pour l'utilisateur
- Connexion permanente au Système d'Information de l'entreprise
- Le tout avec le maximum de sécurité
  - Chiffrement des communications
  - Authentification multi facteurs
  - Contrôle de conformité
  - Contrôle des accès…

Architecture de DirectAccess

(version simplifiée)



Implémentations de DirectAccess

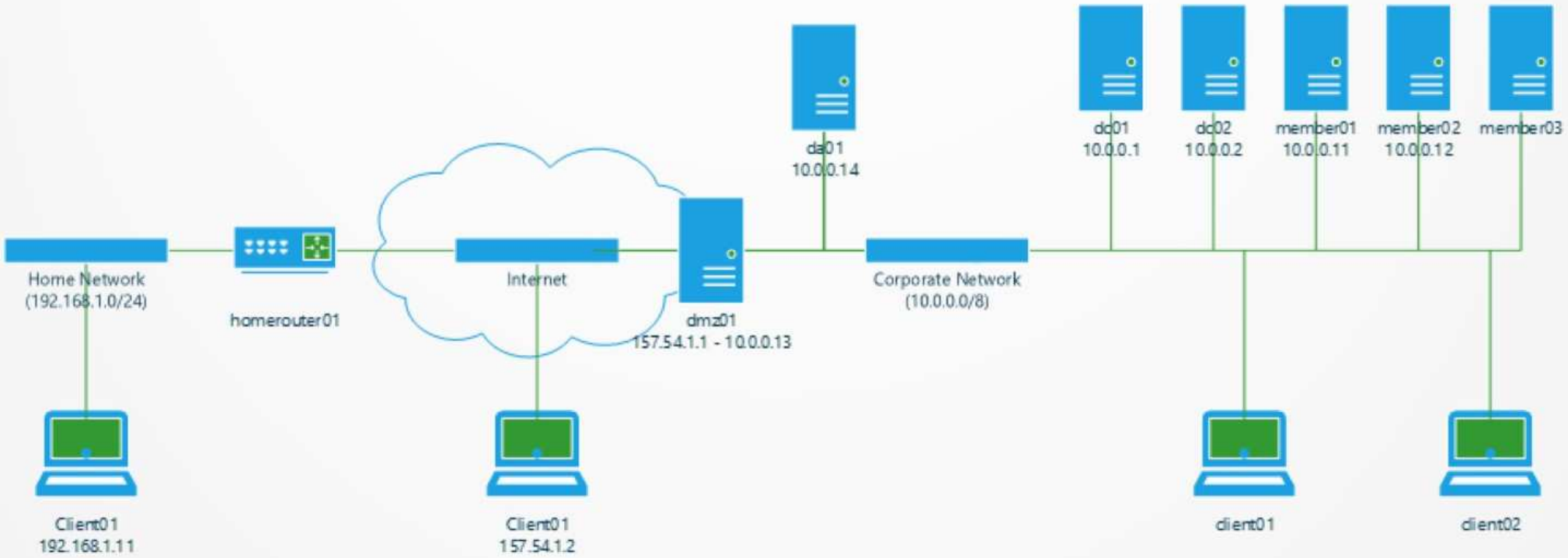
- Première implémentation dans Windows Server 2008 R2
  - Nécessite IPv6 sur le réseau Interne
  - Pas de haute disponibilité
- Deuxième version dans Forefront Unified Access Gateway 2010

DÉPLOIEMENT FACILE

DirectAccess – Assistant au Déploiement simplifié

- Permet de déployer DirectAccess en quelques clics
- Créé automatiquement l'ensemble des objets nécessaires sur l'infrastructure
- Prérequis minimaux:
  - Infrastructure
    - Serveur avec rôle accès distant joint au domaine
    - Accès administratif aux GPO
    - Port forwarding sur NAT (port 443 public vers IP privée du serveur DA)
    - Nom enregistré dans DNS public (qui pointe vers IP public du NAT)
  - Client
    - Windows 8 Entreprise
    - Poste client joint au domaine

Environnement de démonstration



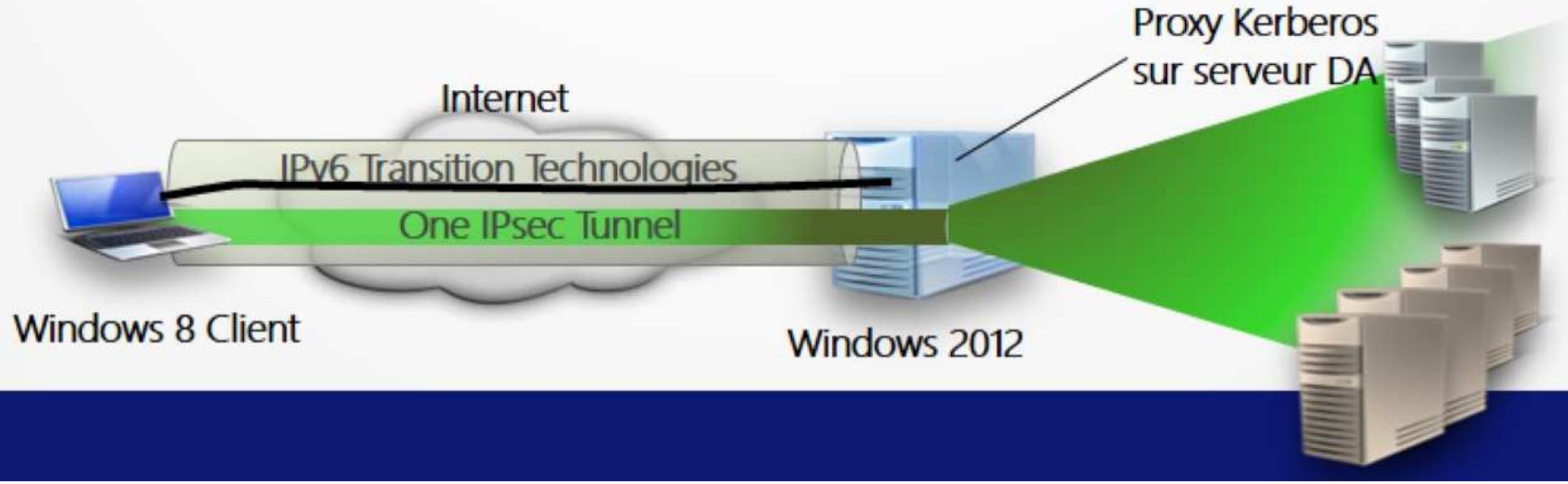
Facilité de déploiement

DirectAccess – Topologies de déploiement

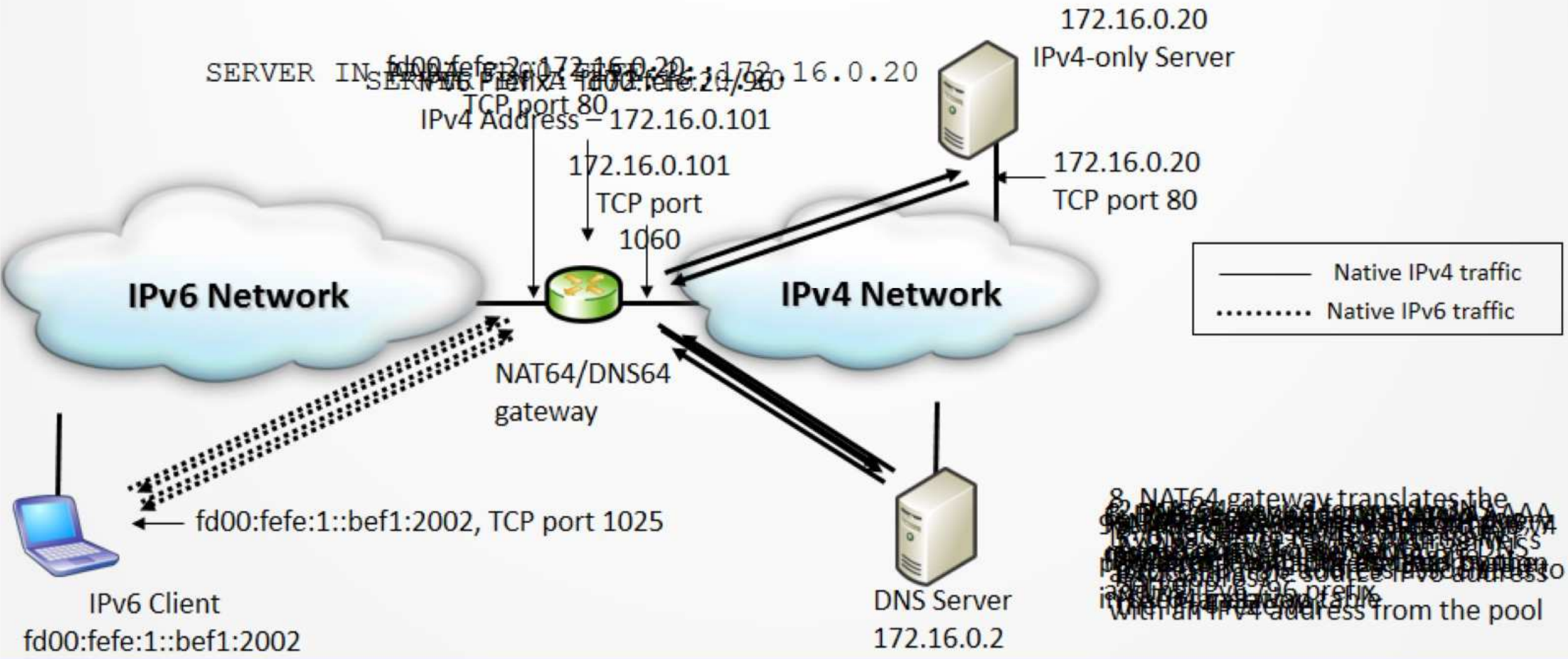
- Serveur derrière une équipement réseau NAT
  - Support de topologie à une carte réseau
- Sans Infrastructure de clés publiques (PKI)
  - Pas de certificats requis pour les postes clients
  - Création de certificats autosignés pour les serveurs
  - Authentification via « Proxysation » Kerberos du serveur DirectAccess
- Un seul tunnel IPsec
- IPv6 non nécessaire de bout-en-bout

DirectAccess Sans Certificat – Kerberos Proxy

- Authentification Kerberos depuis Internet
  - Pas d'exposition des contrôleurs de domaines à Internet
  - Serveur DirectAccess prend en charge les demandes TGT/TGS via URL du type https://<DirectAccess_ServerFQDN>/KDCProxy
- Spécificité du client Kerberos Windows 8
  - Implémenté pour DirectAccess et Remote Desktop Services



DirectAccess sans IPv6 – NAT64/DNS64



GESTION SIMPLIFIEE

Accès distants unifiés

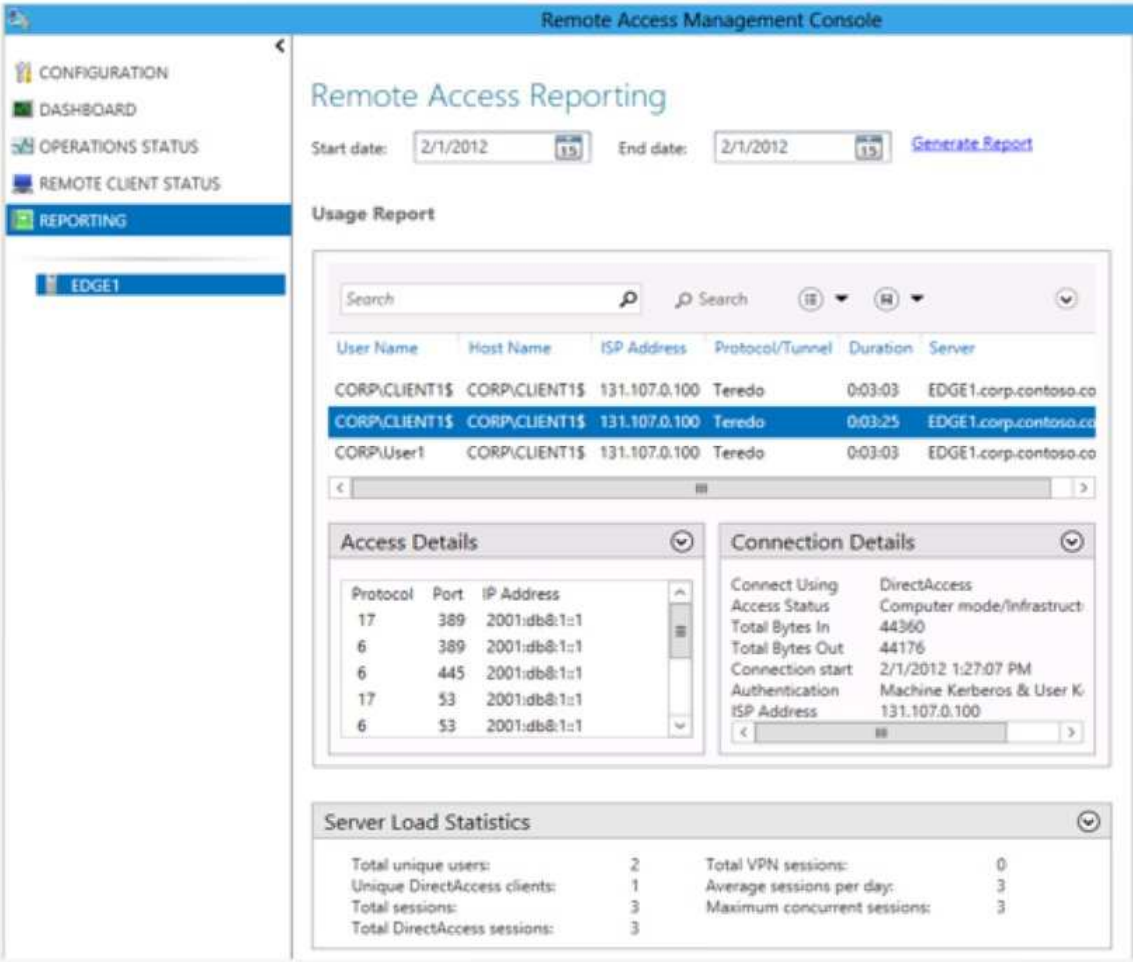
- Console de gestion des accès distant centralisée
  - Vue d'entreprise sur l'ensemble des services d'accès distants
- Serveur DirectAccess et VPN supportés sur la même machine
  - Gérés dans la même console
  - Création automatique du client VPN
- Support de la configuration VPN Site-à-Site
  - Intégration de IKEv2 dans la suite de protocoles S2S

Surveillance et opérations

- Console Accès Distant offre surveillance avancée de l'état
  - Opération des différent composants
  - Fraicheur de la configuration
  - Offre une vue globale « Entreprise »
- Surveillance proactive disponible avec Management Pack pour Operations Manager 2012 SP1
  - Rôle RemoteAccess

Historisation des connexions

- Affichage centralisée de la configuration et de l'état de santé
  - Surveillance des éléments de santé des serveurs DirectAccess
- Historisation des connexions
  - Vision des connexions instantanées
  - Historique des connexions conservé



Contexte Powershell

- Tout est réalisable en Powershell côté serveur comme côté client
- Serveur, installation :
  - Install-RemoteAccess -NoPrerequisite -DAInstallType FullInstall -InternetInterface "Private Internet" -InternalInterface "Private Corpnet" -ConnectToAddress "edge1.contoso.com"
- Client, vérifications :
  - Get-DnsClientNrptPolicy
  - Get-NCSIPolicyConfiguration
  - Get-DAConnectionStatus
  - Get-DAClientExperienceConfiguration

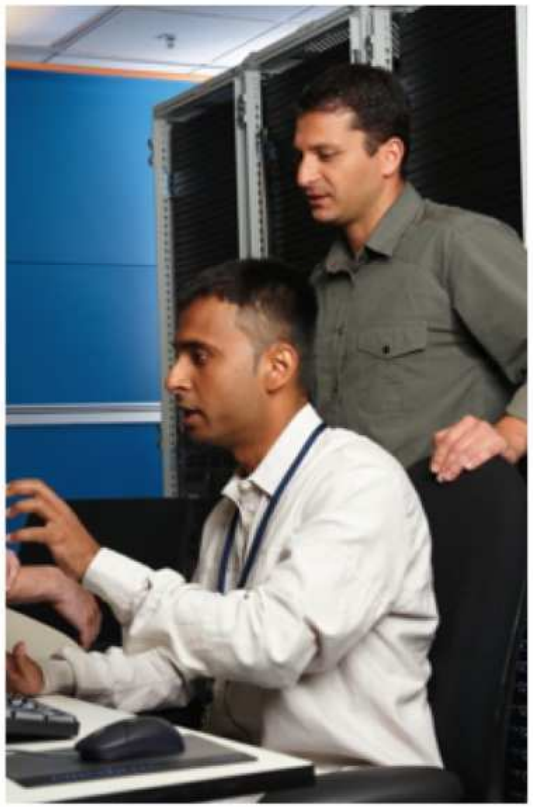
Performance et montée en charge

Support de fermes de serveurs

Déchargement materiel IPsec dans les machines virtuelles

Améliorations des IO dans les machines virtuelles avec SR-IOV

Optimisations d'IP-HTTPS



Haute disponibilité des serveurs DirectAccess

- Support de Windows Network Load Balancing pour DA et VPN
  - Supporte jusqu'à 8 nœuds
- Assistant de déploiement de configuration IP
  - Pas besoin d'administrer NLB en dehors de DA
- Supporte l'utilisation de matériel (HLB)
  - Avec l'application des articles de KB 2782560 et 2788525

Optimisations matérielles

- SR-IOV
  - Single Root – IO Virtualization, accès direct à la carte réseau sans passer par couches de virtualisation
- IPsec Offload
  - Fonctionalités matérielles exposées dans les VM
  - Activer via Set-NetAdapterIPsecOffload –Name Interface –Enabled TRUE
- UDP et RSS
  - Support de la répartition du trafic UDP sur tous les cœurs CPU

Optimisations pour IP-HTTPS

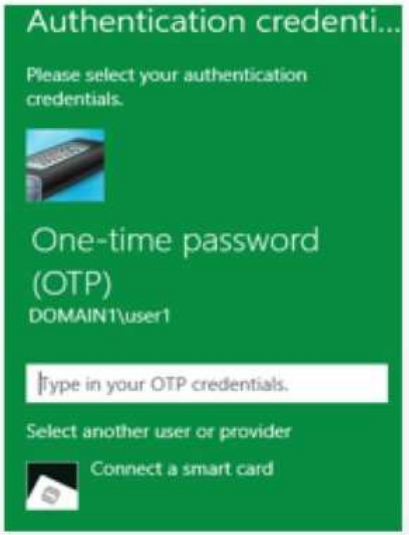
- Auto découverte des proxy
- Support des proxy avec authentification
- Suppression de la double encapsulation (IP-HTTPS NULL)
- Quelques ajustements sur tailles de buffers, gestion des locks, etc.
- IP-HTTPS désormais le protocole de transition favoris (mode UFBPS)

Migrations et supports des clients

- Migration in-place depuis Windows Server 2008R2 supportée
- Migration complète depuis UAG 2010 SP1
  - En mode side-by-side
- Infrastructure WS 2012 sait gérer clients :
  - Windows 8 Entreprise
  - Windows 7 Entreprise
    - Mode simplifié complet non supporté:
      - Possible d'accéder en IP-HTTPS uniquement
      - Besoin de certificats clients
      - Pas de multisite – clients attachés à un site

Expérience utilisateur sur Windows 8

- DirectAccess est inclus dans la barre de gestion des réseaux
- Méthodes d'authentification: Kerberos, PKI, carte à puce (physique ou virtuelle)
- Etat facilement visible dans barre réseaux

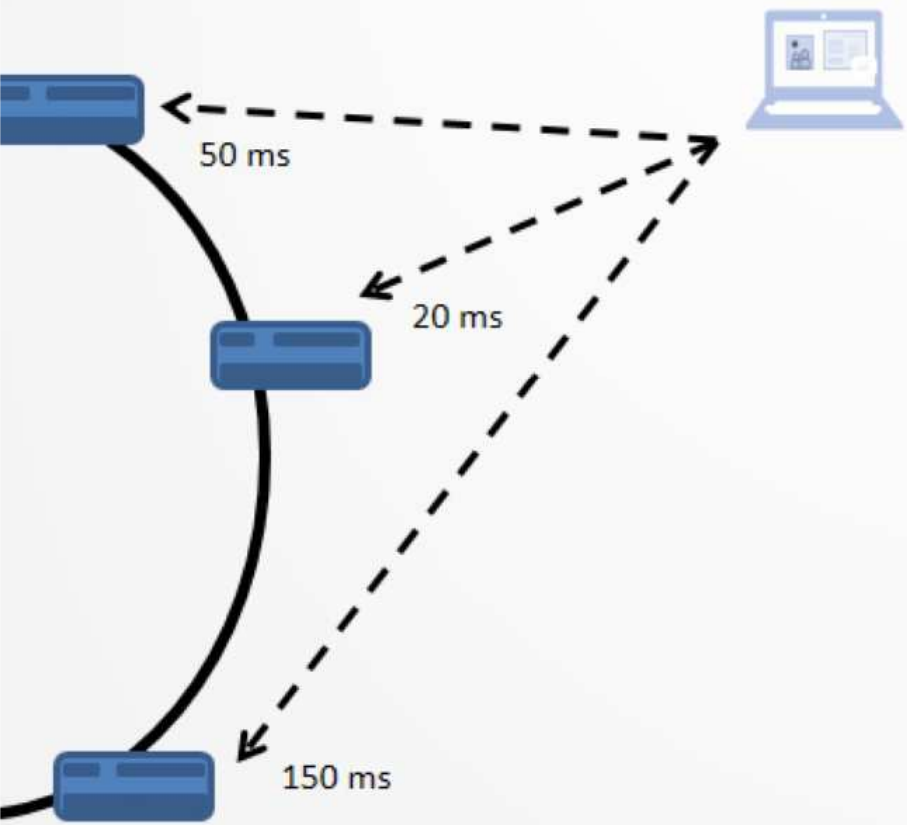


NOUVEAUX SCÉNARIOS

Nouveautés de WS 2012

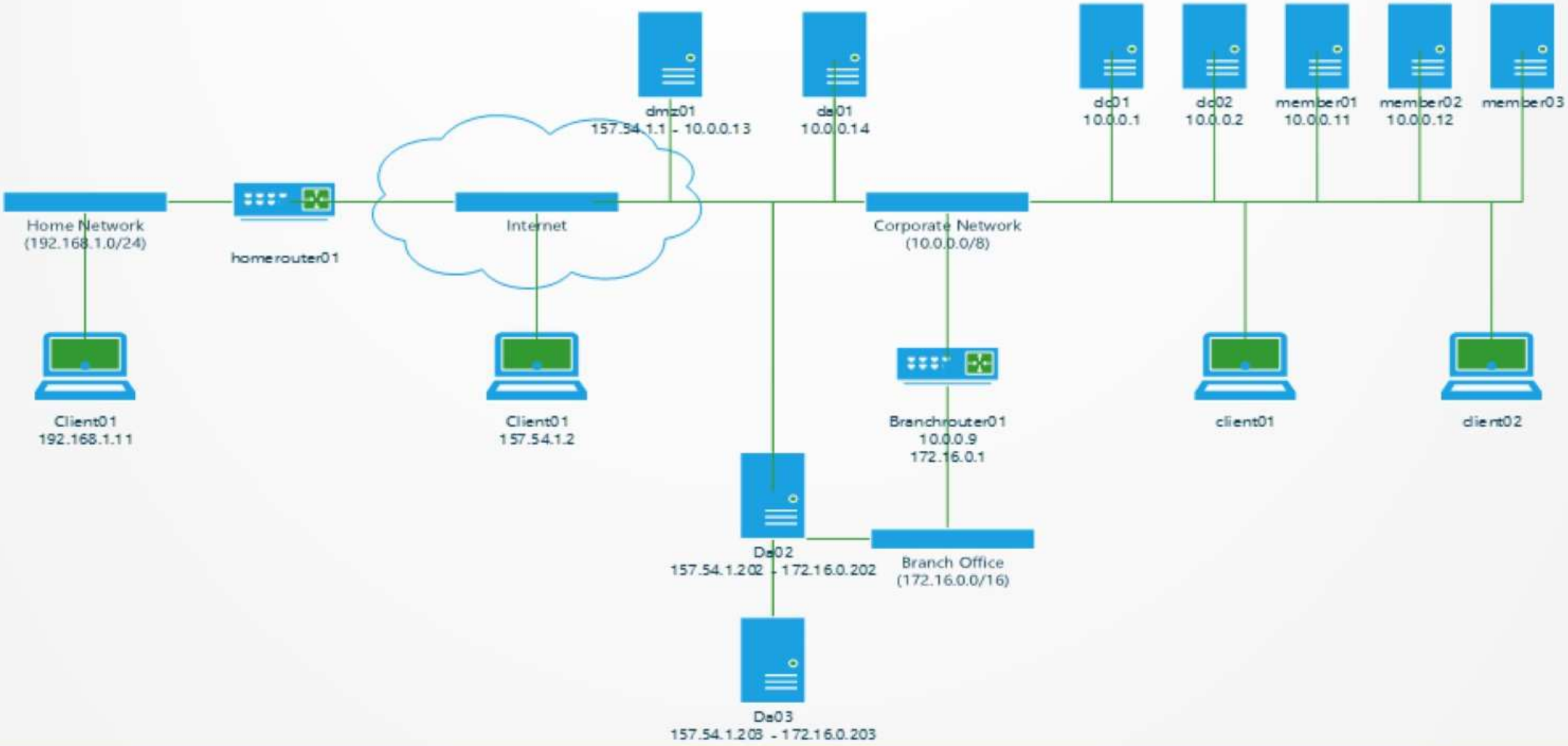
- Intégration de fonctionnalités exposées par UAG :
  - Network Access Protection
  - One Time Passwords
  - Configuration du Force Tunneling
  - Mode Gestion uniquement
  - Support de multiples domaines

Gestion des points d'entrées multiples



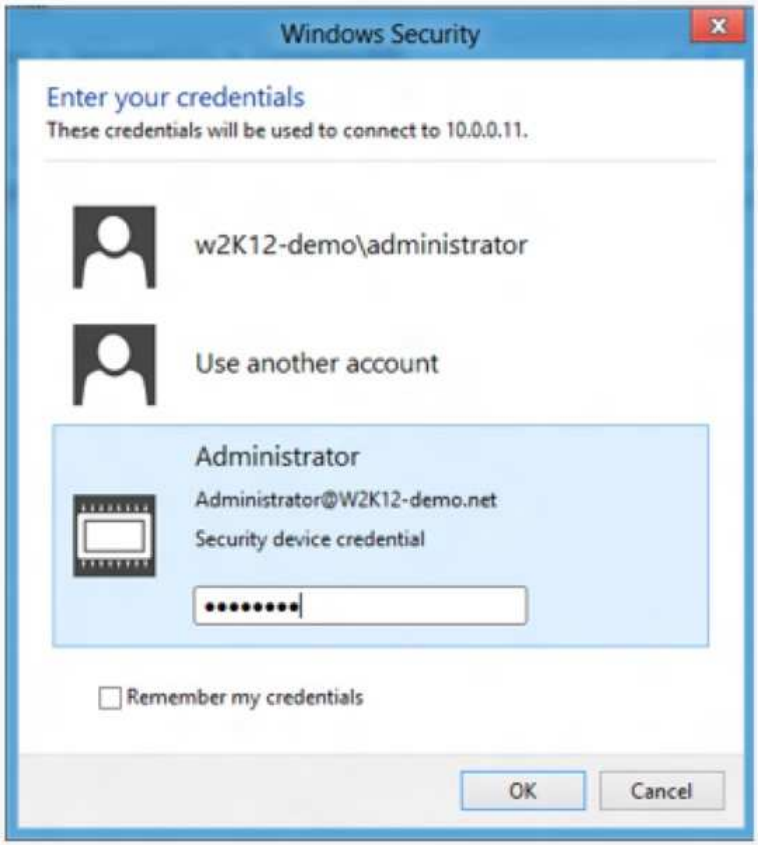
- Détection automatique du point d'entrée le plus proche
  - Basée sur la latence des points d'entrées
  - Clients Windows 7 utilisent un point d'entrée fixe
- Support de Global Server Load Balancing

Environnement de démo

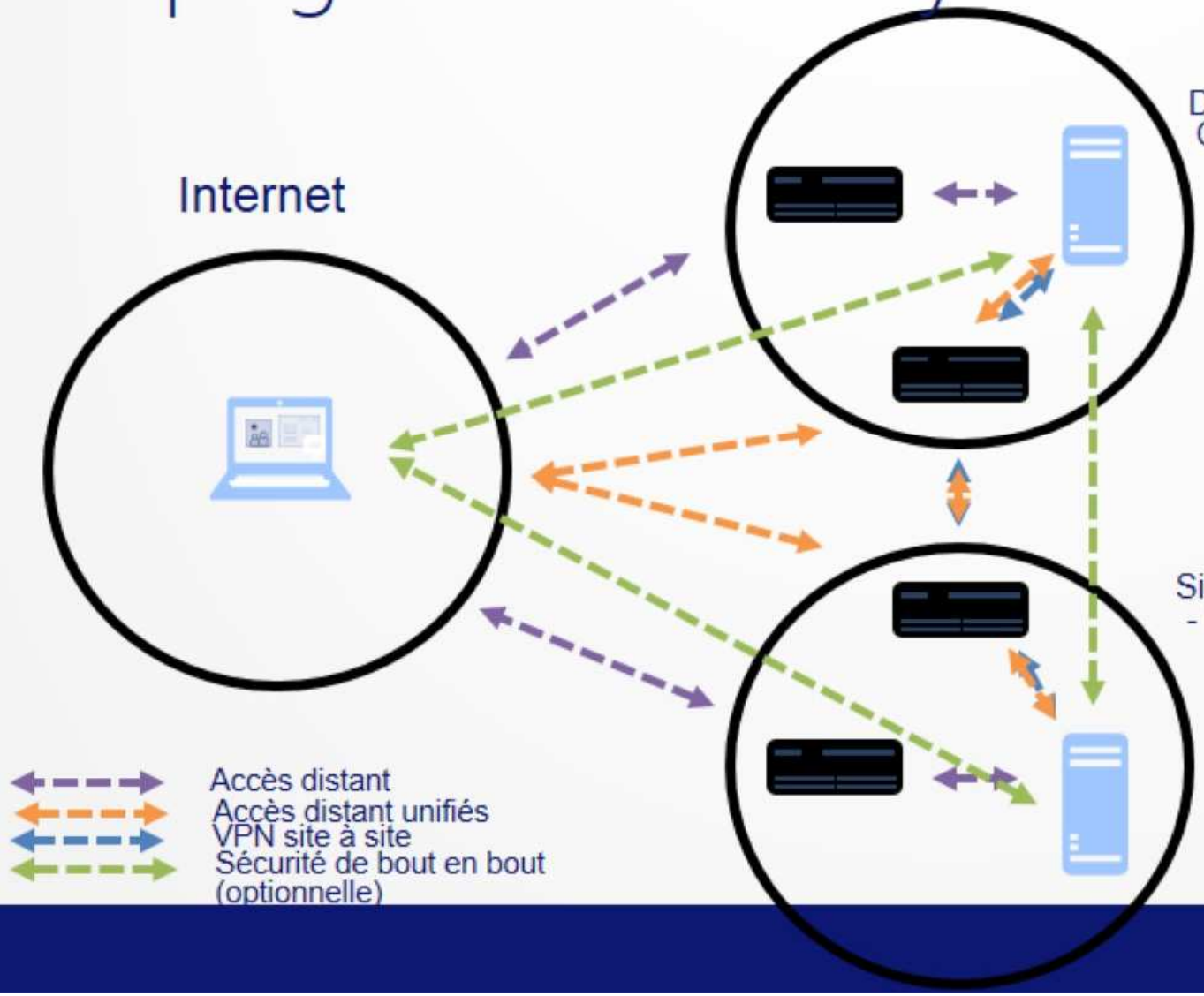


Virtual SmartCard

- Possibilité de faire de l'authentification à 2 facteurs :
  - Certificat
  - Code PIN
- Carte à puce virtuelle utilisant la sécurité du TPM (1.2 et >)
- Déploiement assez simple
- Parfaitement adapté aux tablettes



Toplogie avec cloud hybride



DirectAccess et VPN:
Accès distant:
Connexion en utilisant une infra dédiée
- non gérée

Gestion des connexions pour tous les types de machines - gérées

Site-to-Site:
Connexion en utilisant une infra dédiée

Ajout au domaine « hors-ligne »

- Permet de joindre une machine au domaine sans accès immédiat au domaine
  - Introduit dans Windows7/Windows Server 2008 R2
  - Inclus désormais les GPO et les certificats
- Etapes:
  - Création du compte machine et appartenance aux groupes DA
  - Création du blob
  - Application sur la machine cliente
- Compatible avec Windows To Go

Etapes de l'ajout au domaine « hors-ligne »

- Etapes :
  1. Création du compte machine et appartenance aux groupes DA
     - New-ADComputer –name Arnaud1
     - Add-ADPrincipalGroupMembership –Identity Arnaud1 –Memberof <DNofDAClientsSG> -Server <DCtoRun>
  2. Création du blob
     - Djoin /provision /domain <your domain name> /machine <remotemachinename> /policynames <DAClientGPOname> /rootcacerts /savefile c:\provision\provision.txt /reuse
     - Ou /certtemplate <certTemplateName>
  3. Application sur la machine cliente
     - Djoin /requestodj /loadfile C:\provision\provision.txt /windowspath %windir% /localos

Nouveautés DirectAccess de Windows Server 2012

Facilité de déploiement

- Déploiement et configuration simplifiée
- Couts d'infrastructure et de déploiement moindres
- Pas d'IPv6 sur le réseau d'entreprise
- Déploiement en mode gestion-uniquement
- Support du déploiement derrière une NAT

Gestion

- Gestion centralisée avec le VPN
- Surveillance disponible dans la console d'administration
- Journalisation des accès distants intégré
- Interface de gestion PowerShell
- Interface utilisateur simple et intégrée à Windows

Performance et montée en charge

- Meilleure montée en charge et support du NLB/HLB
- Meilleurs performances dans les environnements virtualisés et accélérations matérielles
- Optimisations de l'encapsulation IP-HTTPS

Nouveaux scénarios

- Support multisite, avec une seule console de gestion
- One-time password (OTP)
- Provisionning hors ligne
- Support de topologies de clouds hybrides

Conclusion DirectAccess Windows Server 2012

- Déploiement rapide, simple, évolutif
- Administration efficace à l'échelle de l'entreprise
- Nouveaux scénarios pour permettre un fluidité et sécurité accrue

→ Plus d'excuse pour ne pas déployer rapidement ☺